

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH)
OF A LENOVO IDEAPAD 5 LAPTOP,)
AN NXT 128 GB USB DRIVE AND)
A PHILIPS USB DRIVE IN THE)
CUSTODY OF HOMELAND)
SECURITY INVESTIGATIONS,)
275 CHESTNUT ST, MANCHESTER,)
NEW HAMPSHIRE

Case No. 20-mj- 216-01-AJ _____

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Shawn Serra, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, being duly sworn, do depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant authorizing a search of a Lenovo Ideapad 5 laptop computer, and two USB hard drives, all of which were seized from Karl Peterson and are currently in the custody of Homeland Security Investigations, 275 Chestnut Street, Manchester, New Hampshire (“the Devices”). I seek authority to search the Devices and extract from them electronically stored information that constitutes evidence, fruits, and instrumentalities of criminal violations which relate to the possession and distribution of child pornography, as described in Attachment B.

2. I have been employed as an HSI Special Agent since June of 2005, and am currently assigned to the Manchester, New Hampshire Resident Office. I graduated from the University of Massachusetts, Lowell, Massachusetts with a Bachelor of Science Degree in Criminal Justice. In 2003, I graduated from the University of Massachusetts, Lowell, Massachusetts with a Master of Arts Degree in Criminal Justice. I have also received training in

the areas of child sexual exploitation including violations pertaining to possession and production of child pornography by attending a twenty-three-week training program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. I am A+ Certified which is an entry level certification in the Information Technology industry, I have attended Basic Computer Evidence Recovery Training (BCERT) and I am a Certified Forensic Computer Examiner (CFCE) through the International Association of Computer Investigative Specialists (IACIS). As part of my duties, I have observed and reviewed examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, to include digital/computer media.

3. I am a “Federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. The information contained in this affidavit is based on information conveyed to me by other law enforcement officials, and my review of records, documents and other physical evidence obtained during this investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have set forth all material information but have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Specified Federal Offenses are presently located on the Devices.

5. I submit that the facts set forth in this affidavit establish probable cause to believe that violations of 18 U.S.C. §§ 2252(a)(2) (receipt/distribution of child pornography) have been committed by Karl Peterson and that there is probable cause to believe that evidence and fruits, and instrumentalities of violations of that crime, as set forth below, will be found on the Devices.

STATUTORY AUTHORITY

6. This investigation concerns an alleged violation of 18 U.S.C. § 2252(a)(2), related to the distribution of child pornography in the District of New Hampshire. Section 2252(a)(2) makes it a crime for any person to knowingly distribute any visual depiction using any means or facility of interstate or foreign commerce if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

7. “Child pornography” includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

8. “Sexually explicit conduct” is defined by 18 U.S.C. § 2256(2)(A) as “actual or simulated (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal . . . ; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person.”

9. Not every display of the genitals or pubic area qualifies as “lascivious exhibition.” In deciding whether the display of the genitals or pubic area is a “lascivious exhibition,” the following factors may be considered: (1) whether the genitals or pubic area are the focal point of the display; (2) whether the setting is sexually suggestive, for example, a setting traditionally associated with sexual activity; (3) whether the child’s pose is unnatural or her attire

inappropriate, taking her age into consideration; (4) whether the child is fully or partially nude; (5) whether the display suggests sexual coyness or a willingness to engage in sexual activity; and (6) whether the display appears designed or intended to elicit a sexual response from the viewer.

10. "Minor" means any person under the age of 18 years. 18 U.S.C. § 2256(1).

11. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image; and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. 18 U.S.C. § 2256(5).

PROBABLE CAUSE

12. In November 2020, Special Offender Specialist (SOS) Steven Seero of the United States Probation and Pretrial Services (USPPS) in the District of New Hampshire, provided your affiant with the following information.

13. On December 15, 2011, Peterson was sentenced to 120 months of incarceration, and 3 years of supervised release for possession of child pornography.

14. On January 15, 2020, Peterson violated the terms of his original supervised release and was sentenced to an additional 6 months of incarceration and a lifetime term of supervised release. Part of those conditions included the following:

You must submit your person, property, house, residence, vehicle, papers, computers (as defined in 18 U.S.C. § 1030(e)(1)), other electronic communications or data storage devices or media, or office, to a search conducted by a United States Probation Officer. Failure to submit to a search may be grounds for revocation of release. You must warn any other occupants that the premises may be subject to searches pursuant to this condition. The probation officer may conduct a search under this condition only when reasonable suspicion exists that you have violated a condition of supervision and that the areas to be searched You

must allow the probation officer to install computer monitoring software on any computer (as defined in 18 U.S.C. § 1030(e)(1)) you use. You must pay for the cost of this monitoring software to the extent you are able, as determined by the probation officer. Any search must be conducted at a reasonable time and in a reasonable manner.

15. On June 16, 2020, Peterson began his second term of supervised release.

16. In October 2020, Peterson obtained permission from SOS Seero to purchase a Lenovo Ideapad laptop. On October 7, computer monitoring software (RemoteCOM¹) was installed on Peterson's computer pursuant to the above-noted special condition.

17. On November 3, 2020, at approximately 7:00 a.m., SOS Seero received a phone call from Dean Friedrich, an employee of RemoteCOM. Dean advised that he had been alerted by another staff member at Remotecom that Peterson's computer had searched "video sex with child" and "sexually abused young girls vaginas (sp)" on his monitored computer. SOS Seero then logged into the RemoteCOM officer portal where he checked Peterson's computer activity from November 1-3, 2020. SOS Seero observed screenshots taken from Peterson's computer which displayed what appeared to be child and adult pornography. Additionally, he observed screenshots which appeared to show Peterson chatting online using a web application "DALnet." Peterson appeared to be using two screen names in these chats, "PervMan" and "Childfckr45." One of the chat rooms was titled "Welcome to Dalnet's Teen Sex Chat!!" and the screen shots showed Peterson's computer conversing with other users and downloading/uploading files to the chat. Additionally, from the screenshots taken of Peterson's computer, it appeared as if whomever was using the computer was saving and/or accessing files, including the child pornography files, to an external drive. In some

¹ RemoteCOM is the name of a software company contracted by the United States Probation Office to conduct computer monitoring of persons under supervision. The company employs staff to monitor certain activity that may be captured by a monitored computer, and it populates an online database with contents such as screenshots for U.S. Probation Officers to view.

screenshots he could see the “D” drive active in the screen shots, indicative of the user saving or accessing files to/from an external drive. SOS Seero also observed screenshots of the following:

- A pre-pubescent female with her legs being held open by another person and an adult male rubbing or sexually penetrating the female’s anus.
- A pre-pubescent female with what appeared to be an adult penis inserted into her anus.
- An adult female performing cunnilingus on a prepubescent female.
- A juvenile female touching the penis of an adult male.
- Several nude females on a bed, one appeared approximately 2-4 years old, three others appeared approximately 5-8 years old, and one of the 5-8 year old nude females is fondling the penis of and straddling an adult male.

18. On November 3, 2020, SOS Seero met with Peterson at his residence. During that meeting, SOS Seero seized Peterson’s Lenovo Ideapad, an NXT USB drive, a Philips USB drive, and a receipt, all of which were found in his apartment pursuant to a search that was conducted under the authority of the aforementioned special condition of supervised release. Peterson admitted to SOS Seero that he had viewed child and adult pornography on his computer on multiple occasions, including on November 1 through 3, 2020. He also admitted that he possessed child pornography on one of the USB drives that SOS Seero had seized. Peterson estimated that the children depicted in the pornography on his USB drive were approximately 8 years old. He further stated that a receipt found in his waste bin was the receipt that documented his purchase of the USB drives that were found in his apartment. Later that day, SOS Seero completed a Petition for Warrant or Summons for Offender Under Supervision, citing two violations of supervised release. The Court then issued a warrant for Peterson’s arrest.

19. On November 12, 2020, your affiant met with SOS Seero and took possession of the devices seized from Peterson's residence and brought them to the HSI Manchester office.

CHARACTERISTICS COMMON TO INDIVIDUALS WHO POSSESS OR PRODUCE

CHILD PORNOGRAPHY

20. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who view and/or possess, receive, and/or produce images of child pornography:

- a. Individuals who possess, receive, and/or produce child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity. Individuals who have a sexual interest in children or images of children typically retain such images for many years.
- b. Likewise, individuals who possess, receive, and/or distribute child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer or smartphone. These child pornography images are often maintained for several years and are kept close by, to enable the individual to view the child pornography images, which are valued highly.
- c. Individuals who possess, receive, and/or distribute child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of

names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Forums, such as chat rooms, bulletin boards, newsgroups or IRC chat rooms have forums dedicated to the trafficking of child pornography images.

21. I know, based on my training and experience, that people who have a demonstrated sexual interest in children and child pornography often maintain collections of images of child pornography. I am therefore requesting authority to search the Devices for evidence of child pornography or any communication involving the abuse of children, and evidence relating to the production, possession, and distribution of any child pornography or child exploitation material.

22. As with most digital technology, communications made from a computer or cellular phone are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP (Internet Service Provider) client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been

deleted, they can be recovered months or years later using readily available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

23. I also know that electronic devices store evidence that can inform investigators who used the Device, when, and how it was used.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

25. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

26. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

27. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

28. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

29. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how

the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

31. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

32. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

33. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

34. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

35. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices

consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

37. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

38. Based on the foregoing, there is probable cause to believe contraband, evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252 (receipt/distribution of child pornography) will be found on the Devices described in Attachment A. I respectfully request that this Court issue a search warrant for the Devices, authorizing the seizure and search of the items described in Attachment B.

/s/ Shawn Serra
Special Agent Shawn Serra
Department of Homeland Security
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Nov 23, 2020

Time: 10:38 AM, Nov 23, 2020

Andrea K. Johnstone
Andrea K. Johnstone
United States Magistrate Judge
District of New Hampshire



ATTACHMENT A

The property to be searched includes a Lenovo Ideapad laptop, an NXT USB drive, and a Philips USB drive, all seized from Karl Peterson and currently in the custody of Homeland Security Investigations, 275 Chestnut Street, Manchester, New Hampshire (“the Devices”).

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the Devices described in Attachment A that relate to violations of 18 U.S.C. § 2252 (distribution of child pornography) including:

1. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, e-mail messages, chat logs, electronic messages, or other digital data files) pertaining to the distribution, production and possession of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
2. In any format and medium, all originals, computer files, and copies of child pornography as defined in 18 U.S.C. § 2256(8), child exploitation material, visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), images or videos of children showering or using the bathroom, or child erotica.
3. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the owner of the Devices for the purpose of receiving, sending, or discussing child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) concerning child pornography or membership in online groups, clubs, or services that provide or make accessible child pornography to members.
5. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
6. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, e-mail messages, chat logs, electronic messages, and other digital data files), pertaining to use or ownership of the Device described above.

7. Any and all documents, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.